Appendix C

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

March 17, 2016

Alert Number
I-031716-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

MOTOR VEHICLES INCREASINGLY VULNERABLE TO REMOTE EXPLOITS

This PSA is a joint product by the Federal Bureau of Investigation, the Department of Transportation and the National Highway Traffic Safety Administration.

As previously reported by the media in and after July 2015, security researchers evaluating automotive cybersecurity were able to demonstrate remote exploits of motor vehicles. The analysis demonstrated the researchers could gain significant control over vehicle functions remotely by exploiting wireless communications vulnerabilities. While the identified vulnerabilities have been addressed, it is important that consumers and manufacturers are aware of the possible threats and how an attacker may seek to remotely exploit vulnerabilities in the future. Third party aftermarket devices with Internet or cellular access plugged into diagnostics ports could also introduce wireless vulnerabilities.

Modern motor vehicles often include new connected vehicle technologies that aim to provide benefits such as added safety features, improved fuel economy, and greater overall convenience. Aftermarket devices are also providing consumers with new features to monitor the status of their vehicles. However, with this increased connectivity, it is important that consumers and manufacturers maintain awareness of potential cyber security threats.

Vehicle hacking occurs when someone with a computer seeks to gain unauthorized access to vehicle systems for the purposes of retrieving driver data or manipulating vehicle functionality. While not all hacking incidents may result in a risk to safety – such as an attacker taking control of a vehicle – it is important that consumers take appropriate steps to minimize risk. Therefore, the FBI and NHTSA are warning the general public and manufacturers – of vehicles, vehicle components, and aftermarket devices – to maintain awareness of potential issues and cybersecurity threats related to connected vehicle technologies in modern vehicles.

How are computers used in modern motor vehicles?

Motor vehicles contain an increasing number of computers in the form of electronic control units (ECUs). These ECUs control numerous vehicle functions from steering, braking, and acceleration, to the lights and windshield wipers. A wide range of vehicle components also have wireless capability: from keyless entry, ignition control, and tire pressure monitoring, to diagnostic, navigation, and entertainment systems. While manufacturers attempt to limit the interaction between vehicle systems, wireless communications, and diagnostic ports, these new connections to the vehicle architecture provide portals through which adversaries may be able to remotely attack the vehicle controls and systems. Third-party devices connected to the vehicle, for example through the diagnostics port, could also introduce vulnerabilities by providing connectivity where it did not exist previously.

What are some of the ways an attacker can access vehicle networks and driver data?

Vulnerabilities may exist within a vehicle's wireless communication functions, within a mobile device – such as a cellular phone or tablet connected to the vehicle via USB, Bluetooth, or Wi-Fi – or within a third-party device connected through a vehicle diagnostic port. In these cases, it may be possible for an attacker to remotely exploit these vulnerabilities and gain access to the vehicle's controller network or to data stored on the vehicle. Although vulnerabilities may not always result in an attacker being able to access all parts of the system, the safety risk to consumers could increase significantly if the access involves the ability to manipulate critical vehicle control systems.

Example: Recently Demonstrated Remote Exploits

Over the past year, researchers identified a number of vulnerabilities in the radio module of a MY2014 passenger vehicle and reported its detailed findings in a whitepaper published in August 2015.[a] The vehicle studied was unaltered and purchased directly from a dealer. In this study, which was conducted over a period of several months, researchers developed exploits targeting the active cellular wireless and optionally user-enabled Wi-Fi hotspot communication functions. Attacks on the vehicle that were conducted over Wi-Fi were limited to a distance of less than about 100 feet from the vehicle. However, an attacker making a cellular connection to the vehicle's cellular carrier – from anywhere on the carrier's nationwide network – could communicate with and perform exploits on the vehicle via an Internet Protocol (IP) address.

In the aforementioned case, the radio module contained multiple wireless communication and entertainment functions and was connected to two controller area network (CAN) buses in the vehicle. Following are some of the vehicle function manipulations that researchers were able to accomplish.

- In a target vehicle, at low speeds (5-10 mph):
  - Engine shutdown
  - Disable brakes
  - Steering
- In a target vehicle, at any speed:
  - Door locks
  - Turn signal
  - Tachometer
  - Radio, HVAC, GPS

What did the manufacturer in the recent case do to fix or mitigate the identified vulnerabilities?

In this case, NHTSA believed the vulnerability represented an unreasonable risk to safety based on a number of critical factors: once exploited, the vulnerability allowed access to and manipulation of critical vehicle control systems; the population of vehicles potentially at risk was huge; and the likelihood of exploitation was great given that the researchers were scheduled to publish the bulk of their work product. As a result, almost one and a half million vehicles were recalled (NHTSA Recall Campaign Number: 15V461000). Before the researchers' report was released, the cellular carrier for the affected vehicles blocked access to one specific port (TCP 6667) for the private IP addresses used to communicate with vehicles. However, the recall was still necessary to mitigate other, short-range vulnerabilities.

The manufacturer and cell service provider have provided a remedy to mitigate the specific vulnerabilities. The manufacturer announced it would notify owners of vehicles affected by the recall and would mail them a USB drive containing the update and additional security features for the vehicle software. Alternatively, the manufacturer announced that owners could visit a Web site to check if their vehicle was included in the recall and to download the software update to a USB drive. Owners who did not wish to install the update via USB to their own vehicles were given the option to have their vehicle dealer install the update.

Cybersecurity Recalls and Consumer Action

How can consumers determine whether their vehicle has been recalled for a vehicle cybersecurity issue?

When a vehicle is included in a recall, the manufacturer sends a notification to vehicle owners informing them of the issue and how to obtain a free remedy to address the problem.

In general, it is important that consumers maintain awareness of the latest recalls and updates affecting their motor vehicles. This can be done by following the instructions on NHTSA's safercar.gov Web site, media and news announcements of recalls, contacting your nearest vehicle dealership, or checking the vehicle manufacturer's Web site for recall-related information. Vehicle owners should check the vehicle's VIN for recalls at least twice per year using this Web link: http://vinrcl.safercar.gov

Consumers can also look for other related information for their vehicles at the following Web links:

http://www-odi.nhtsa.dot.gov/owners/SearchSafetyIssues http://www.recalls.gov/nhtsa.html

How can consumers help minimize vehicle cybersecurity risks?

1. Ensure your vehicle software is up to date

If a manufacturer issues a notification that a software update is available, it is important that the consumer take appropriate steps to verify the authenticity of the notification and take action to ensure that the vehicle system is up to date.

As a note of caution, if manufacturers regularly make software updates for vehicles available online, it is possible that criminals may exploit this delivery method. A criminal could send socially engineered e-mail messages to vehicle owners who are looking to obtain legitimate software updates. Instead, the recipients could be tricked into clicking links to malicious Web sites or opening attachments containing malicious software (malware). The malware could be designed to install on the owner's computer, or be contained in the vehicle software update file, so as to be introduced into the owner's vehicle when the owner attempts to apply the update via USB. Additionally, an attacker could attempt to mail vehicle owners USB drives containing a malicious version of a vehicle's software. To mitigate potential risks, vehicle owners should always:

- Verify any recall notices received by following the steps for determining whether a vehicle has been recalled for a vehicle cyber security issue, as outlined above.
- Check on the vehicle manufacturer's Web site to identify whether any software updates have been issued by the manufacturer.
- Avoid downloading software from third-party Web sites or file-sharing platforms.
- Where necessary, always use a trusted USB or SD card storage device when downloading and installing software to a vehicle.
- Check with the vehicle dealer or manufacturer about performing vehicle software updates.

If uncomfortable with downloading recall software or using recall software mailed to you, call your dealer and make an appointment to have the work done by a trusted source.

2. Be careful when making any modifications to vehicle software

Making unauthorized modifications to vehicle software may not only impact the normal operation of your vehicle, but it may introduce new vulnerabilities that could be exploited by an attacker. Such modifications may also impact the way in which authorized software updates can be installed on the vehicle.

3. Maintain awareness and exercise discretion when connecting third-party devices to your vehicle

All modern vehicles feature a standardized diagnostics port, OBD-II, which provides some level of connectivity to the in-vehicle communication networks. This port is typically accessed by vehicle maintenance technicians, using publicly available diagnostic tools, to assess the status of various vehicle systems, as well as to test emissions performance. More recently, there has been a significant increase in the availability of third-party devices that can be plugged directly into the diagnostic port. These devices, which may be designed independent of the vehicle manufacturer, include insurance dongles and other telematics and vehicle monitoring tools. The security of these devices is important as it can provide an attacker with a means of accessing vehicle systems and driver data remotely.

While in the past accessing automotive systems through this OBD-II port would typically require an attacker to be physically present in the vehicle, it may be possible for an attacker to indirectly connect to the vehicle by exploiting vulnerabilities in these aftermarket devices. Vehicle owners should check with the security and privacy policies of the third-party device manufacturers and service providers, and they should not connect any unknown or un-trusted devices to the OBD-II port.

4. Be aware of who has physical access to your vehicle

In much the same way as you would not leave your personal computer or smartphone unlocked, in an unsecure location, or with someone you don't trust, it is important that you maintain awareness of those who may have access to your vehicle.

What should you do if you suspect you are a victim of vehicle hacking?

In much the same way as you would not leave your personal computer or smartphone unlocked, in an unsecure location, or with someone you don't trust, it is important that you maintain awareness of those who may have access to your vehicle.

1. Check for outstanding vehicle recalls or vehicle software updates

It is important that you check to identify whether there are any outstanding recalls related to your vehicle. This can be done by following the steps outlined above. You may also check on the manufacturer's Web site to determine whether there are any software updates that may need to be applied.

2. Contact the vehicle manufacturer or authorized dealer

An important step is being able to diagnose whether any anomalous vehicle behavior might be attributable to a vehicle hacking attempt. Contact your vehicle manufacturer or authorized dealer and provide them with a description of the problem so that they can work with you to resolve any potential cyber security concerns.

3. Contact the National Highway Traffic Safety Administration

In addition to contacting the manufacturer or authorized dealer, please report suspected hacking attempts and perceived anomalous vehicle behavior that could result in safety concerns to NHTSA by filing a Vehicle Safety Complaint.

- https://www-odi.nhtsa.dot.gov/VehicleComplaint/.

4. Contact the FBI

In addition to the above steps, please reach out to your local FBI field office and the Internet Crime Complaint Center (IC3).

- FBI field office contacts can be identified at https://www.fbi.gov/contact-us/field.
- You can file a complaint with the IC3 at http://www.ic3.gov. Please provide any relevant information in your complaint.

Agency and Industry Action

What is NHTSA doing on vehicle cyber security?

NHTSA is the regulatory agency that sets and enforces the federal motor vehicle safety standards for new vehicles. They are actively working on several initiatives to improve the cyber security posture of vehicles in the United States. More information about their vehicle cyber security activities can be found at:

http://www.nhtsa.gov/staticfiles/administration/pdf/presentations_speeches/20
VehicleCybersecurity_07212015.pdf

What are automakers doing on vehicle cyber security?

In addition to the steps taken by individual automakers to address vehicle safety and security, the auto industry has established an Information Sharing and Analysis Center (ISAC) to provide a trusted mechanism for exchanging cyber security information. The Auto ISAC will act as a central hub for gathering intelligence to help the industry analyze, share, and track cyber threats. Automakers are also collaborating on best practices for enhancing the cyber resiliency of motor vehicle electronics and associated in-vehicle networks.

---

a Online research paper; Chris Valasek, Charlie Miller; IOActive Security Services Technical Whitepaper; "Remote Exploitation of an Unaltered Passenger Vehicle"; 10 August 2015; http://www.ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf; 17 September 2015. IOActive is a computer security services company. Authors have researched vehicle vulnerabilities for several years.↩